IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Criminal No. 1:17-CR-00154 (TSE)**
	)	
KEVIN PATRICK MALLORY,	)	
	)	
Defendant	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S SECOND SUPPLEMENTAL MEMORANDUM IN AID OF SENTENCING

COMES NOW the United States and submits this brief in response to Defendant Kevin Patrick Mallory's Second Supplemental Memorandum in Aid of Sentencing ("Def. 2d Supp. Memo"). In his most recent filing, Defendant directs the Court's attention to the recent plea agreement in *United States v. Hansen*, 1:18-CR-00057-DB. [Dkt. 250] While the government finds very little to agree with in defense counsel's characterization of the *Hansen* case, it does agree with the defense's understatement that "there are distinctions between" that case and the one at bar. *See* Def. 2d Supp. Memo at 1. While both Hansen and Defendant are former Defense Intelligence Agency ("DIA") employees, both of whom found themselves embroiled with suspected intelligence officers from the People's Republic of China Intelligence Service ("PRCIS"), the cases are dissimilar in almost every other aspect.

1. Defendant Has Never Accepted Responsibility for his Crimes

Ron Hansen was charged with attempted passage of national defense information ("NDI"), in violation of 18 U.S.C. § 794; acting as an agent of a foreign government in the United States without prior notification to the Attorney General, in violation of 18 U.S.C. § 951; violations of export control laws; and certain other crimes ancillary to those charges. *See Hansen* Indictment

(Ex. 1). The first, and most crucial, difference between Hansen and Defendant is that Hansen accepted responsibility for his actions—and did so without delay—in the form of pleading guilty to attempted passage of NDI. The plea the government entered into with Hansen reflects this acceptance of responsibility. Because of Hansen's prior work for the United States intelligence community ("USIC") and the nature of espionage cases, the government expected to brief and argue issues related to classified information during Classified Information Procedures Act ("CIPA") litigation. Hansen's timely plea saved the government significant resources and avoided exposure of classified information at trial.[1] It is only with this early acceptance of responsibility and avoidance of the risk of disclosure of classified information that the government agreed to a 180-month sentence,[2] which is still 60 months (five years) longer than that proposed by defense counsel in the instant case. *See* Def. 2d Supp. Memo at 2 (asking the Court impose no longer than 120 months' imprisonment).

Conversely, to this day, Defendant has yet to accept any responsibility whatsoever for his actions. Defendant pushed the case against him through time-consuming CIPA litigation to a public trial. Because Defendant did not accept responsibility pre-trial,[3] the government had to disseminate sensitive national information to lay jurors in order to meet its burden at trial. Additionally, officials from multiple government agencies took time away from their duties in support of the national security to appear at trial in this matter.

---

1 The only CIPA filing in the Hansen case was the government's *ex parte* filing pursuant to CIPA Section 4.

2 Hansen has not yet been sentenced, and will not be until September 2019.

3 To be clear, the government is not arguing that Defendant should be punished for exercising his right to go to trial. To the contrary, Defendant had an absolute right to a jury trial in this case, he chose to assert that right, and he was afforded a full and fair trial. But having exercised that right, Defendant cannot now claim that his case should be viewed in the same light as someone like Hansen, who accepted responsibility early.

2. Defendant Successfully Passed Classified Information to the Chinese Intelligence Officers

The second difference involves the compromise of what happened with the classified information in each case. The government did not allege that Hansen successfully passed NDI to the PRCIS. As reflected in the Indictment and plea agreement, the charged violation of 18 U.S.C. § 951 was not based on Hansen's passage of classified information. *See, e.g.*, *Hansen* Indictment ¶¶ 8, 32-34, 37, 40-43 (Hansen attended conferences pursuant to PRCIS taskings and provided non-public information provided at those conferences) (Ex. 1); *Hansen* Plea at 4 (Ex. A to Def. 2d Supp. Memo [Dkt. 250]) (information passed included that "gathered at various industry conferences").

The classified information at issue in *Hansen* was SECRET information that a cooperating, confidential human source ("CHS") provided to Hansen as part of a law enforcement operation in which the classified material was kept in a controlled setting and both the CHS and Hansen were under close surveillance by the FBI. Because Hansen was dealing with a CHS as part of a covert law enforcement operation, there was minimal risk the classified information would be provided to unauthorized persons. And it never did.

In this case, however, there is no doubt that, as part of his conspiracy with a Chinese intelligence officer to commit espionage, Defendant did pass classified information to the PRCIS. The substance of Defendant's communications with Michael Yang, a PRCIS intelligence officer, confirms as much. *See, e.g.*, GX 8-6, Row 17 (conversation regarding transmitted document "no1"). The log files on the covert communications ("covcom") device Defendant used to message Yang similarly confirm that, at a minimum, Defendant successfully passed to Yang a classified table of contents and a white paper classified at the SECRET level. GX 8-21 (covcom log files).

3. Defendant Attempted to Pass TOP SECRET Information as Part of this Conspiracy

Further, in comparing the *Hansen* case to Defendant's, Defendant wholly ignores the difference in the classification of the information at issue and the resulting consequences for sentencing. As noted, the material underlying the offense of conviction in *Hansen* involved information classified at the SECRET level that was never passed to a foreign government. Here, conversely—in addition to the SECRET information Defendant successfully passed to the PRCIS—Defendant completed all of the necessary steps to transmit additional information classified at the SECRET *and* TOP SECRET levels from Defendant's WeChat account to Yang's WeChat account. *See* GX 8-21; Testimony of James Hamrock, May 31, 2017 ("Hamrock Tr."), at 359-372. In fact, Defendant hit send four separate times for one document, Document No. 4, classified at the TOP SECRET level. Hamrock Tr. at 381:5-8. Information may only be classified as TOP SECRET if its unauthorized disclosure "reasonably could be expected to cause *exceptionally grave damage* to the national security." Executive Order 13526 § 1.2(a)(1) (emphasis added). Indeed, Central Intelligence Agency ("CIA") Original Classification Authority ("OCA") Nancy Morgan testified that this document was particularly sensitive because it dealt with human sources who "could be at risk of harm" should the information be disclosed to an adversary of the United States. Morgan Tr. at 801:3-6 (Ex. 2).[4]

The sentencing guidelines appropriately take into account the difference in damage that can result from passage of information classified at the SECRET and TOP SECRET levels; TOP SECRET information results in a base offense level of 42, whereas SECRET information results in 37. *See* U.S.S.G. § 2M3.1. As a result, the agreed-upon sentence of 180 months for Hansen is

[4] Defendant's conduct was particularly egregious because he himself had been responsible for these human assets during his time at DIA, and he elected to swap this information regarding his former assets for money *after* learning that those former assets had pending travel to the PRC. GX 8-21; GX 3-26; *see also* Testimony of Robert Ambrose, June 5, 2017, at 862:15-17.

at the *high end* of the 151-188 month range following his acceptance of responsibility. On the other hand, as further described below, Defendant's guideline range is life imprisonment.

4. Defendant Abused His Position of Trust and Obstructed Justice

Unlike Defendant, Hansen was not charged with attempting to provide information he had access to during his time as a clearance holder between 2002 and 2011. *See Hansen* Indictment ¶ 17 (Ex. 1) (Hansen last held a security clearance in 2011). Rather, Hansen attempted to cultivate a connection to a *current* security clearance holder to obtain information that might be of value to the Chinese. Since Hansen was not seeking to pass classified information he had as a result of his prior security clearance, the government did not seek an enhancement for abuse of a position of trust. Hansen was also not charged with false statements made to investigating Federal Bureau of Investigation ("FBI") agents and the government did not advocate for a corresponding obstruction of justice enhancement.

Here, Defendant qualifies for both enhancements as the government noted in its position on sentencing. *See* Government's Position on Sentencing, Sept. 14, 2018 ("Gov't Position Memo"), at 3-5, and 9-15 [Dkt. 211]. Because Defendant conspired to pass TOP SECRET information taken during his time as an active clearance holder, thereby abusing his position of trust, and obstructed justice to do so, his Guidelines calculation is life in prison.

CONCLUSION

For the foregoing reasons, there is simply no comparison between Defendant's conduct and that of Hansen, who accepted responsibility early and attempted to pass SECRET, not TOP SECRET information. As further described in the Government's prior sentencing submissions, the sentence calculated pursuant to the United States Sentencing Commission's Guidelines—namely, lifetime imprisonment—is the appropriate sentence in this case.

Dated April 2, 2019

Respectfully submitted,

G. Zachary Terwilliger
United States Attorney

By: /s/ Jennifer K. Gellie
JENNIFER KENNEDY GELLIE
Trial Attorney
National Security Division
United States Department of Justice
950 Pennsylvania Ave., NW
Washington, D.C. 20530
Tel.: (202) 233-0785
Fax: (202) 233-2146
Jennifer.Gellie@usdoj.gov

JOHN T. GIBBS
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700
Fax: 703-299-3981
John.Gibbs@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that I have caused an electronic copy of the *GOVERNMENT'S RESPONSE TO DEFENDANT'S SECOND SUPPLEMENTAL MEMORANDUM IN AID OF SENTENCING* to be served via ECF upon counsel for Defendant Kevin Patrick Mallory.

By: /s/

John T. Gibbs
Virginia Bar No. 40380
Assistant United States Attorney
United States Attorney's Office
2100 Jamieson Avenue
Alexandria, Virginia 22314
Phone: 703-299-3700
Fax: 703-299-3981

EXHIBIT 1

JOHN W. HUBER, United States Attorney (No. 7226)
ROBERT A. LUND, Assistant United States Attorney (No. 9579)
KARIN FOJTIK, Assistant United States Attorney (No. 7527)
ALICIA H. COOK, Trial Attorney, U.S. Department of Justice (No. 8851)
MARK K. VINCENT, Assistant United States Attorney (No. 5357)
PATRICK T. MURPHY, Trial Attorney, U.S. Department of Justice (MD Bar)
ADAM L. SMALL, Trial Attorney, U.S. Department of Justice (NY Bar #2750602)
Attorneys for the United States of America
111 South Main Street, Suite 1800
Salt Lake City, Utah 84111
Telephone: (801) 524-5682

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH, NORTHERN DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. RON ROCKWELL HANSEN, Defendant.	Case No. **INDICTMENT** COUNT 1, 18 U.S.C. § 794(a)- Attempt to Gather or Deliver Defense Information; COUNT 2, 18 U.S.C. § 951- Agent of a Foreign Government; COUNTS 3 - 5, 31 U.S.C. § 5332 – Bulk Cash Smuggling; COUNTS 6 - 13, 31 U.S.C. § 5324 – Structuring Monetary Transactions; COUNTS 14 & 15, 18 U.S.C. § 554 - Smuggling Goods from the United States; Case: 1:18-cr-00057 Assigned To : Benson, Dee Assign. Date : 6/20/18 Description: USA v. Hansen

THE GRAND JURY CHARGES:

BACKGROUND

At all times material to this Indictment:

The United States Intelligence Community

1. The United States Intelligence Community (USIC) consisted of U.S. executive branch agencies and organizations that worked separately and together to conduct intelligence activities related to foreign relations and the protection of the national security of the United States.

2. The U.S. Department of Defense (DoD) was a U.S. executive branch agency tasked with providing military forces needed to deter war and to protect the security of the United States.

3. The Defense Intelligence Agency (DIA) was a component of DoD and the USIC, which collected (including through classified means), analyzed, produced, and disseminated foreign intelligence and counterintelligence to support national and DoD missions. The DIA planned, managed, and executed intelligence operations during times of peace, crisis, and war. The DIA provided defense-related intelligence for the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, combatant commanders, other DoD components, and non-DoD agencies. Furthermore, the DIA conducted administrative and technical support activities within and outside the United States as necessary for cover arrangements. The USIC also included U.S. Army Intelligence, another DoD component.

4. The FBI was a U.S. government intelligence and law enforcement agency and was a component of the USIC. The FBI was responsible for, among other things, conducting counterintelligence investigations and activities.

Classified Information

5. National security information constituted information owned by, produced by, produced for, and under the control of the United States government that related to the conduct of foreign relations or the national defense. Pursuant to Executive Order 13526 and its predecessors, national security information corresponded to three possible classification levels:

a. Information was classified as TOP SECRET if the unauthorized disclosure of that information reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority was able to identify and describe.

b. Information was classified as SECRET if the unauthorized disclosure of that information reasonably could be expected to cause serious damage to the national security that the original classified authority was able to identify and describe.

c. Information was classified as CONFIDENTIAL if the unauthorized disclosure of that information reasonably could be expected to cause damage to the national security that the original classified authority was able to identify and describe.

6. Only individuals determined eligible by an appropriate U.S. government official could lawfully access classified information. Additional requirements dictated that such an individual sign an approved non-disclosure agreement, receive a security clearance, and possess a "need to know" the classified information. Those authorities further required the storage of classified information in an approved facility and container commensurate with its classification level.

7. Classification markings represented the usual means of communicating the need to protect classified national security information. Classified documents typically contained banners on the top and bottom stating the highest level of classification and any additional controls associated

with the materials, as well as markings relating to the information contained in each paragraph.

8. In addition to classification markings, classified information at times contained dissemination markings which restricted the distribution of the information. These markings include "NF" or "NOFORN" dissemination control markings that stood for "No Foreign Dissemination." The NOFORN marking denoted a limitation to disseminate the information only to U.S. persons.

The People's Republic of China Intelligence Services

9. The People's Republic of China intelligence services (PRCIS) encompassed both the civilian and military components of Chinese intelligence programs. Civilian intelligence agencies included the Ministry of State Security (MSS) and the Ministry of Public Security (MPS). The MSS consisted of a central ministry, provincial state security departments, and municipal state security bureaus, such as the Beijing State Security Bureau (BSSB) and the Shanghai State Security Bureau (SSSB). The MPS was the principal domestic police and security agency.

10. The MSS maintained primary responsibility for domestic counterintelligence, foreign intelligence, and aspects of political and military security. Among other things, the MSS and its regional bureaus focused on identifying and influencing the foreign policy of other countries, including the United States. The MSS and its bureaus sought to obtain information on military, political, economic, and security policies that might affect the People's Republic of China (PRC), foreign intelligence operations directed at the PRC, and biographical profiles of foreign politicians and intelligence officers. Much of the PRC's espionage efforts in industrialized nations focused on acquiring technology that may or may not have been cleared for export. The PRCIS commonly used agents running front companies to purchase high-technology equipment.

11. PRCIS human source operations tended to originate inside the PRC, where the PRCIS preferred to meet with its sources or assets. The PRCIS recruited individuals with direct and second-hand access to information. The PRCIS recruited, among others, individuals who traveled in and out of the PRC for business or study and who could return to their home country to gain employment in the national security system or exploit existing connections. The PRCIS commonly used money to recruit sources.

The Defendant

12. Ron Rockwell Hansen (HANSEN), a United States (U.S.) citizen, resided in Syracuse, Utah. HANSEN retired from the U.S. Army (Army) as a Warrant Officer with a background in signals intelligence and human intelligence. HANSEN spoke Mandarin-Chinese and Russian. From approximately 2000 to 2006, while serving on active duty in the Army, HANSEN worked as an intelligence case officer for the DIA. He retired from the Army in early 2006 after more than 20 years of service. Upon retirement, DIA hired HANSEN as a civilian intelligence case officer. While on active duty with the Army and while employed as a DIA civilian, HANSEN possessed a TOP SECRET security clearance.

13. As part of the training to become a case officer, HANSEN received training in managing assets, deterring surveillance, avoiding detection, and handling classified and sensitive information.

14. HANSEN eventually resigned from DIA in December 2006, after which he became a member in two companies, H-11 Digital Forensics Company LLC and H-11 Digital Forensics Services LLC (hereinafter referred to collectively as H-11). HANSEN's primary responsibilities related to H-11's business in Asia. From approximately 2007 until late 2011, HANSEN maintained office space and an apartment in the PRC. He traveled frequently from Utah to the

PRC.

15. According to HANSEN, he partnered with two PRC nationals, whom he identified by anglicized names as "Amy" and "Robert," at his H-11 office in Beijing. According to HANSEN, Robert maintained close connections to numerous contacts within PRCIS agencies.

16. From approximately the end of 2000 until late 2011, HANSEN performed work for the U.S. government that provided HANSEN with additional access to classified national defense information. During his military service, the U.S. government entrusted HANSEN with access to sensitive government materials, including closely held national defense information and classified documents and materials.

17. Between 2000 and 2011, HANSEN signed multiple agreements that he would not disclose his work with the U.S. government or the information derived from that relationship. Over his many years of holding security clearances, HANSEN received training regarding classified information, including the definitions of classified information, the levels of classification, as well as the proper handling, marking, transportation, and storage of classified materials. HANSEN received training on his duty to protect classified materials from unauthorized disclosure, which included complying with handling, transportation, and storage requirements. HANSEN received instruction that the unauthorized transportation and storage of classified materials risked disclosure and that transmission of the information could endanger the national security of the United States and the safety of its citizens.

18. As a prerequisite to accessing classified information during his employment with the U.S. government agencies, HANSEN signed numerous contracts containing non-disclosure agreements in which he acknowledged both the harm that could result from the unauthorized disclosure of classified information and the applicability of criminal espionage laws should he

make an unauthorized disclosure of such information or should he unlawfully retain such information.

19. Beginning in early 2012, HANSEN attempted to regain access to national defense information by seeking positions of employment or confidence with USIC agencies, often through former DIA associates.

a. In February of 2012, HANSEN approached U.S. Army Intelligence, through a former DIA associate, and offered to work as a double agent against the PRCIS.

b. In May of 2012, HANSEN applied for a position with DIA.

c. In mid-2013, in a meeting at DIA Headquarters facilitated by a high-ranking DIA officer, HANSEN suggested to a DIA analyst assigned to a classified program targeting the PRC that DIA operate HANSEN as a source.

d. In November of 2013, when HANSEN's efforts to gain access through those intelligence agencies failed, HANSEN approached another component of the U.S. Army Intelligence through another former DIA associate.

e. In February of 2015, HANSEN approached the FBI and offered to work as a double-agent against the PRCIS.

f. In September of 2015, HANSEN contacted a United States House of Representatives member assigned to the House Permanent Select Committee on Intelligence, and HANSEN proposed that he work as a member of the Representative's staff on intelligence issues.

g. In May of 2016, as set forth in more detail below, HANSEN reestablished contact with a current DIA case officer. In later meetings, HANSEN encouraged that DIA case officer to use HANSEN as a source against the PRCIS.

20. At no time did HANSEN notify the Attorney General of the United States that he was acting as an agent for any foreign government, including the PRC.

21. According to HANSEN's financial records and his admissions to the FBI, between 2011 and 2016, the following companies employed HANSEN after his work with the U.S. government ended:

Company	**Company Description**	**HANSEN's Role**	**Employment Dates** *(based on Payroll Checks)*
Logicube	Computer Forensics Hardware Manufacturer	Director of Worldwide Sales	September 2011 – July 2012
Smith Electric Vehicles	Electric Vehicle Design and Production	Contractor	July 2014 – March 2016

22. According to HANSEN's financial records and business registration records, HANSEN possessed an ownership interest in the following entities:

Entity	**Description**	**Business Address**	**Initial Registration Date**	**HANSEN's Role**	**Account Signatory**	**Main Account**
AC-FPS Business Group LLC	American Chinese Friendship Promotion Society	57 W 200 S Suite 302 Salt Lake City,UT	March 26, 2013	Owner	Yes	Wells Fargo x6750
H-11 Digital Forensics Services LLC	Computer Forensics Company	57 W 200 S Suite 302 Salt Lake City,UT	July 9, 2007	Chief Executive Officer/ Owner	Yes	Wells Fargo x3972
H-11 Digital Forensics Company LLC	Computer Forensics Company	57 W 200 S Suite 302 Salt Lake City,UT	November 20, 2006	Chief Executive Officer/ Owner	Yes	Wells Fargo x8498 x1000
Nuvestack LLC	Cloud Computing Company	600 17th St Denver, CO	November 19, 2013	Owner	Yes	Wells Fargo x0702
Nuvestack Inc.	Cloud Computing Company	57 W 200 S Suite 302 Salt Lake City,UT	September 25, 2015	Owner	Yes	Wells Fargo x4721

23. Nuvestack provided cloud computing and information technology services. American and Chinese Friendship Promotion Society Business Group (AC-FPS) sought to provide professional and business services in the PRC.

24. Between September of 2012 and June 2, 2018, HANSEN had only intermittent periods of verifiable income. HANSEN's military pension, which paid approximately $1,900 in net monthly income, constituted his only consistent source of income.

25. According to jointly-filed, personal tax returns for tax years 2013 through 2016, HANSEN claimed large losses from his affiliated partnerships, including Nuvestack, AC-FPS, and H-11, resulting in less than $40,000 in his gross adjusted income reported each year. For tax years 2013-2016, AC-FPS recorded business losses each year. Nuvestack filed its initial U.S. Return of Partnership Income for tax year 2013 and claimed $0.00 income and $64,002 in expenses. According to Nuvestack's U.S. Return of Partnership Income for tax year 2014, business losses claimed were -$1,114,889 with only $4,000 in gross receipts. Nuvestack failed to file taxes in 2015 and 2016 and carried significant debt.

26. In addition to the financial strain caused by his ownership interests, between 2012 and June 2, 2018, HANSEN's personal unsecured debt ranged from $150,000 to $200,000. HANSEN exhausted his own credit limit and, as of late 2016, HANSEN began to borrow funds against credit cards belonging to his family members.

Meetings with the FBI

27. In 2014, the FBI commenced an investigation into HANSEN's activities. Throughout 2015, while unaware of the pending investigation, HANSEN participated in nine voluntary meetings with FBI agents in Salt Lake City, Utah. HANSEN claimed that he initiated the meetings with the FBI to offer his cooperation as a source. During those meetings, HANSEN

described numerous encounters with PRCIS officials, and HANSEN disclosed that agents of the PRCIS targeted him for recruitment.

28. HANSEN told the FBI that, by at least early 2014, he began meeting with two MSS officers known to him as "David" and "Martin." HANSEN described meeting with David and Martin in private rooms in tea houses and hotels in Beijing, and explained that Robert set up those meetings. HANSEN related that during a business trip to the PRC in early 2015, David and Martin offered him $300,000 per year in exchange for providing "consulting services." HANSEN reported that David and Martin asked him to attend conferences or exhibitions on forensics, information security, and military communications and to conduct product research. HANSEN stated that David and Martin gave him money by overpaying him for purchases of computer forensic products.

29. In March of 2015, when asked how he could obtain information for the PRCIS, HANSEN told the FBI that he "could start going to Washington, D.C. and meeting with friends who are in the intelligence community and try and elicit classified info from them." However, HANSEN acknowledged that doing so would constitute "alerting behavior." Physical surveillance and court-authorized intercepted phone calls confirm that HANSEN began reaching out to former DoD and DIA associates that same year and continuing into 2016. Several of those associates had not had contact with HANSEN in many years.

30. In June and July of 2015, HANSEN gave the FBI two thumb drives containing several reports that he wrote and other materials he obtained during his work with the U.S. government. When asked by the agents how he safeguarded the material, HANSEN replied that he stored the material on external drives and maintained these drives in a safe in his home. The two thumb drives did in fact contain classified information that HANSEN was not authorized to retain.

31. In December of 2015, in the final meeting with FBI agents, HANSEN reiterated his potential value to the PRCIS, suggesting the PRCIS could direct him to contact two specific DIA case officers in Texas and Georgia. At the conclusion of the meeting, FBI agents admonished HANSEN that he must not accept the MSS's offer to work for them. The FBI agents further instructed HANSEN that he must inform the FBI if the PRCIS continued to contact him. At no point thereafter, despite his later admissions to others about his continual meetings with the MSS, did HANSEN report any further interaction with PRCIS to the FBI. As described more fully below, in May of 2016, HANSEN traveled to Texas and met with one of the DIA case officers he mentioned to the FBI in December 2015.

Attending Conferences

32. During the course of the investigation, the FBI learned that HANSEN began attending conferences on behalf of the PRC and its officials as early as 2013 and he continued doing so through 2017. The FBI conducted surveillance of HANSEN at some of those conferences. FBI surveillance personnel observed HANSEN typing notes on his laptop computer and taking photographs of the presenters.

33. From September 9-10, 2015, HANSEN attended the Intelligence & National Security Summit in Washington, D.C. sponsored by the Intelligence and National Security Alliance (INSA) and the Armed Forces Communications and Electronics Association (AFCEA). From April 20-22, 2016, HANSEN attended the AFCEA-sponsored Defense Cyber Operations Symposium in Washington, D.C. From September 7-8, 2016, HANSEN again attended the Intelligence & National Security Summit in Washington, D.C. From November 15-17, 2016, HANSEN attended the AFCEA-sponsored TechNet Asia Pacific Conference in Honolulu, Hawaii. From September 6-7, 2017, HANSEN attended the Intelligence & National Security

Summit in Washington, D.C.

34. Although HANSEN registered for conferences under the name of Nuvestack Inc., he listed his home address rather than the Nuvestack address on registration documents. Recorded phone calls reveal that HANSEN attempted to conceal his attendance at the TechNet conference by asking a close Nuvestack associate not to disclose his location while at the conference. While at the conferences, HANSEN also affirmatively misrepresented to the Nuvestack president and other employees that he had been recalled to military duty.

Searches Related to HANSEN's Travel

35. During the investigation, the FBI also monitored HANSEN's travel. On several instances during the investigation, the FBI enlisted the assistance of officers from U.S. Customs and Border Protection (CBP) to assist with searching and questioning HANSEN as he traveled back to the U.S. from the PRC. Between 2014 and 2017, in each instance that officers from CBP searched HANSEN'S luggage or carry-on baggage, while he cleared customs on his travel back to Utah from the PRC, HANSEN carried U.S. currency and various digital devices, including cellular phones, smart phones, thumb drives, a laptop computer, and/or other digital storage media.

36. HANSEN traveled to the PRC on June 30, 2014 and returned to the U.S. through the Detroit Metropolitan Airport on July 9, 2014. Upon his return, HANSEN knowingly failed to report that he was carrying currency in excess of $10,000, and he failed to complete and submit a Report of International Transportation of Currency or Monetary Instruments (FINCEN Form 105) as required. In Detroit, CBP conducted a secondary inspection of HANSEN's carry-on luggage. When HANSEN realized that CBP intended to search his possessions, HANSEN told the CBP officer that he had failed to declare currency over $10,000. After the interaction with

the CBP officer, HANSEN then disclosed that, in fact, he carried $19,222. HANSEN subsequently completed the required FINCEN Form 105.

37. HANSEN traveled to the PRC on December 5, 2015, and he returned to the U.S. on December 14, 2015. Upon his return, a court-authorized search of HANSEN's carry-on luggage revealed a passcode-protected thumb drive concealed behind a sock in the toe of a shoe. A forensic examination of the thumb drive revealed the file names of photographs and notes related to the September 2015 INSA Summit. The forensic examination also revealed that the thumb drive had been accessed during HANSEN's stay in the PRC. HANSEN's suitcase contained brochures and other materials related to the September 2015 INSA summit. The suitcase also contained a print-out establishing HANSEN's membership in AFCEA starting in June of 2013. HANSEN also carried his MacBook Pro computer and $53,000 in cash. HANSEN told CBP officers that the $53,000 represented proceeds from the sale of a Netwitness server; however, HANSEN could not produce any documentation to verify the sale of the product.

38. On April 18, 2016, during HANSEN's trip to Washington, D.C. to attend the AFCEA conference, the FBI conducted a court-authorized search of HANSEN's hotel room and created a forensic image of HANSEN's MacBook Pro computer. One document found on the computer, saved under the file name "Business Development," contained expenses related to HANSEN's attendance at conferences, his AFCEA membership renewal, and his INSA membership. The Business Development document also contained a list of names and contact information of former DoD/DIA associates of HANSEN. Several of the contacts continued to work for the United States government, including an individual who later began operating as a Confidential Human Source ("CHS"). The Business Development document also included names of U.S. politicians representing the State of Utah. HANSEN did not have any business dealings with the

vast majority of the individuals listed in the document. Additionally, during the forensic examination, the FBI discovered printer file records indicating that, days before his trip to the PRC in December of 2015, HANSEN printed information from LinkedIn related to several former and current DIA case officers.

39. Other documents stored on the computer contained information about conferences that HANSEN previously attended and information about the U.S. military, including information detailing U.S. Cyber Command locations, personnel, and organizational structure.

40. HANSEN traveled to the PRC again on July 17, 2016, and he returned to the U.S. on July 23, 2016. A court-authorized search of HANSEN's luggage when he returned revealed that he carried the same password-protected thumb drive as he had on December 14, 2015. A forensic examination revealed two documents located in the unallocated space on the thumb drive, evidencing an attempt to delete the documents. One document contained notes about the Defense Information Systems Agency, relating to the AFCEA conference HANSEN attended in April of 2016. The examination further revealed that the thumb drive had last been accessed on July 18, 2016, during HANSEN's trip to the PRC.

41. The other document started with an itemized list of expenses related to his May 2016 trip to Texas. The document also contained past and current locations of DIA facilities in San Antonio, as well as cryptic notes related to a classified DIA program and DIA personnel, and cryptic notes about a DIA case officer hiring initiative. The document also contained dates, titles, and locations of upcoming military, intelligence, and technology conferences.

42. HANSEN traveled to the PRC again on December 14, 2017, and he returned to the U.S. on December 19, 2017. Upon his return, during customs processing, the FBI conducted a court-authorized search of HANSEN's luggage and possessions. HANSEN carried a MacBook Air

computer. A forensic examination of the computer revealed a document saved to the computer under the file name "Notes_INSA Summit2016." The document contained several pages of extensive notes about the INSA Summit that HANSEN attended in Washington, D.C. in September of 2016, as well as cryptic notes about his meetings with three former DIA associates during that trip to Washington, D.C.

43. The notes also included expenses related to HANSEN's travel and attendance at the summit in Washington, D.C. The cryptic notes included the initials of the first and last names of the former DIA associates, the dates he met them, and other information likely related to his discussions with them, including cryptic notes related to their employment, such as work with "special ops community" and a specific U.S. government intelligence agency. The cryptic notes also included the initials of the spouse of one of the former DIA associates and the date in July of 2016, when HANSEN had a chance meeting with her while traveling in Japan. At the time, the spouse worked as a DIA employee. The cryptic notes also included the initials of the CHS with an August date, followed by the note "med board," referring to discussions between HANSEN and the CHS about the CHS' medical condition and the CHS' U.S. Army medical board status. The document also contained the date, title, and location of the November 2016 military, intelligence, and technology conference, which HANSEN attended.

HANSEN's Communications with PRCIS

44. HANSEN consistently touted his access to PRCIS intelligence officers throughout the 2015 voluntary meetings with the FBI. As noted above, in February 2015, HANSEN described his ongoing meetings with MSS intelligence officers David and Martin, saying those meetings began in 2014 and continued into 2015. He explained that he stopped traveling to the PRC after December of 2011 while he was applying to return to work with DIA, but he resumed travel in

April of 2013 upon learning he would not be hired. HANSEN described a succession of PRCIS intelligence officers with whom he met during visits to the PRC. He identified one of the officers as Max, who he said later introduced him to David and Martin, with whom he then met exclusively.

45. In the next voluntary meeting with the FBI in March of 2015, HANSEN further described the PRCIS intelligence officer as Max Tong, but said he was unsure if Tong was Max's real last name. HANSEN said he met with Max and Martin in 2013. In the voluntary meeting with the FBI in May of 2015, HANSEN again described various PRCIS intelligence officers with whom he met in the PRC over his years of travel. He admitted to using his personal email accounts, including his @ac-fps.org account, to communicate with certain PRCIS intelligence officers. He provided a sheet of paper with the names and contact information of some of the PRCIS intelligence officers. HANSEN identified Max on the sheet of paper he provided, which listed him as "Max Rain" with an email address @foxmail.com. He again identified Max as the PRCIS intelligence officer who introduced him to MSS intelligence officers David and Martin. In the voluntary meeting with the FBI in September of 2015, HANSEN provided another document listing his PRCIS contacts, including the years of contact and the officers' affiliation. He identified Max Tong as an MSS intelligence officer assigned to "HUMINT," an acronym for Human Intelligence, with a first meeting date of March 2011.

46. A court-authorized search of HANSEN's email account associated with the @ac-fps.org address revealed three email exchanges with Max, using his @foxmail.com email account, during 2012-13. One of HANSEN's email responses to Max included a contact title of "Rain" for the @foxmail.com email address, demonstrating that those email exchanges occurred between Hansen and Max Tong.

47. The emails were sent in mid-2012 and early 2013, and they showed Max's eagerness for HANSEN to resume travel to the PRC. In emails exchanged in July of 2012, HANSEN revealed to Max that he decided to go back to his job at the Department of Defense and he would not be able to travel to the PRC that month. At that time, HANSEN had applied for a position with DIA, which required a security clearance and would have given him renewed access to intelligence reporting. Max sent another email to HANSEN in January of 2013, noting he looked forward to hearing from HANSEN. HANSEN replied in April of 2013, about the time he learned he would not be hired by DIA and right before his first trip back to the PRC since December of 2011, noting he had good news. He wrote that he would be in the PRC the following week, adding that his schedule was busy so they would need to meet early in the morning. He added that he looked forward to seeing Max. HANSEN failed to disclose his ongoing contacts with Max, someone he knew to be a PRCIS intelligence officer, to DIA during his application and security clearance background check investigation.

48. When HANSEN first approached the FBI in February of 2015, he explained that Robert set up his meetings with MSS intelligence officers David and Martin. At a subsequent voluntary meeting with the FBI in March of 2015, when HANSEN again stated that Robert brokered HANSEN's meetings with David and Martin and other PRCIS intelligence officers, the FBI asked HANSEN about Robert's background and why he had direct contact with PRCIS intelligence officers. HANSEN described Robert's access to hundreds of PRCIS officers, adding that Robert visited PRCIS offices, including the MSS office. At a subsequent voluntary meeting with the FBI in September of 2015, HANSEN explained that David and Martin opted to no longer utilize Robert to arrange meetings with HANSEN. They instead gave HANSEN a XINDA-model PRC cell phone with Martin's name and telephone number preprogrammed to

allow HANSEN to communicate directly with Martin to set up in-person meetings after HANSEN arrived in the PRC.

49. The investigation revealed that, as early as July of 2014, HANSEN used various cell phones to communicate with Martin and others in the PRC. HANSEN's use of multiple cell phones to communicate covertly with intelligence officers is consistent with case officer tradecraft training HANSEN received from DIA to communicate securely with human sources.

50. When HANSEN returned from the PRC on July 9, 2014, CBP officers conducted a secondary inspection of HANSEN's luggage and possessions and found an inexpensive NOKIA-brand, PRC cell phone. HANSEN also had a U.S. smartphone.

51. When HANSEN returned from the PRC on December 14, 2015, the FBI conducted a court-authorized search of his luggage and possessions and found an inexpensive XINDA-brand PRC cell phone packed in his carry-on luggage, which he possessed in addition to the U.S. and PRC smartphones he carried in his briefcase. The XINDA phone had call data showing communications with "Martin."

52. Upon HANSEN's return to the U.S. in July 23, 2016, following his travel to the PRC, the FBI conducted another court-authorized search of his luggage and possessions and found an inexpensive NOKIA-brand PRC cell phone packed in his carry-on luggage separate from his U.S. and PRC smartphones located in his briefcase. This NOKIA phone call data showed communications with "Martin." This was not the same NOKIA-brand cell phone found in HANSEN's possession by CBP in July of 2014.

53. On July 11, 2017, the FBI conducted a court-authorized search of HANSEN's checked luggage prior to his flight to the PRC and found HANSEN's Huawei-brand PRC smartphone packed in the luggage. The FBI obtained a forensic image of the phone and found several stored

incoming and outgoing calls and text messages. The forensic image showed HANSEN began using this smartphone during his travel to the PRC in February of 2015, shortly before he contacted the FBI and reported the alleged recruitment pitch by the PRCIS. The forensic image from July 11, 2017 revealed consistent communication to and from a contact identified in the smartphone as "Martin Chen," beginning with HANSEN's trip to the PRC in December of 2016 and including each subsequent trip to the PRC prior to this outbound travel. Those trips occurred in February of 2017, April of 2017, and May of 2017.

54. When CBP questioned HANSEN about the $53,000 in U.S. currency that he declared upon his return travel from the PRC on December 14, 2015, HANSEN explained that he sold a piece of computer forensic equipment to Martin Chen of the MPS. On February 28, 2017, when describing his meetings with the MSS in the PRC, HANSEN told the CHS that the MSS always knows he is coming to the PRC, adding that they do not call themselves the MSS, they call themselves the MPS.

55. During his voluntary meetings with the FBI in 2015, HANSEN explained his extensive interaction with the MPS. The court-authorized search of HANSEN's MacBook Pro computer in April of 2016 revealed photographs saved to the computer depicting HANSEN with uniformed MPS officers, including some in a room with the MPS logo on the wall of the room, confirming admissions he made to the CHS about having ties to the MPS.

56. During a meeting with CHS in April of 2018, as they discussed how they could communicate to avoid detection, HANSEN suggested to CHS they use a covert means of communication using email.

Movement of Money from the PRC to the United States

57. HANSEN did not travel to the PRC during 2012, but he resumed frequent travel to the

PRC in April 2013. Between January of 2013 and June 2, 2018, HANSEN traveled to the PRC 40 times.

58. Since at least April of 2013, HANSEN's return from travel to the PRC coincided with his receipt of large amounts of money. HANSEN moved money from the PRC to the U.S. using three methods: physically carrying cash across the border, Visa card transactions, and wire transfers.

59. Since 2008, Amy and Robert operated a PRC-based entity called Beijing Hua Heng Infosec Company (Infosec) which partnered with H-11 to sell computer forensic products in the PRC. During the partnership, H-11 shipped computer forensic products to Infosec. For example, email correspondence in August of 2013 between HANSEN's @ac-fps.com email account and an email account @h11dfs.com provide shipping details for a product shipped internationally on or about August 8, 2013 from a domestic vendor to Infosec in Beijing. An analysis of bank records revealed that Amy and Robert paid for these products via wire transactions originating from the PRC to H-11 business accounts in the United States. In contrast, beginning in May of 2013, Amy and Robert began wiring funds to an AC-FPS business account controlled by HANSEN on dates that coincided with HANSEN's trips to the PRC.

60. For example, HANSEN traveled to the PRC on August 5, 2013, and he returned to the U.S. on August 27, 2013. On or about August 19, 2013, HANSEN sent an email from his @ac-fps.com email account to Amy and Robert at their @ac-fps.com email accounts asking Robert if he received $15,000 U.S. dollars from HANSEN's driver in the PRC. HANSEN then instructed Robert to send the money to his AC-FPS business account in Utah. On or about August 28, 2013, HANSEN received a $14,985 wire originating from the PRC in his AC-FPS business account.

61. Starting in May of 2013 through June of 2014, HANSEN's travel to the PRC coincided with large cash deposits to HANSEN's personal and business accounts without declarations of currency at the border. In addition, between May of 2013 through September of 2014, Amy and Robert wired funds directly into HANSEN's AC-FPS business account, as set forth in Table 1 below:

TABLE 1: April 2013-June 2014 Travel from the PRC / No Currency Declarations / Deposits

Travel Dates	Customs Declaration	Deposit Date	Amount	Type	Bank Account
April 20 – May 3, 2013	None Portland,OR	May 3, 2013	$4,000	Cash	x4798 Hansen personal
		May 7, 2013	$1,000		
			$12,000		x6750 AC-FPS
		May 13, 2013	$14,985	Wire	
May 26 – June 6, 2013	None Portland,OR	June 6, 2013	$5,000	Cash	x4798 Hansen personal
		June 7, 2013	$14,985	Wire	x6750 AC-FPS
August 5 – August 27, 2013	None Portland,OR	August 28, 2013	$5,500	Cash	x4798 Hansen personal
			$14,985	Wire	x6750 AC-FPS
November 18 – November 26, 2013	None Seattle,WA	November 26, 2013	$9,000	Cash	x4798 Hansen personal
		November 29, 2013	$10,000		x6750 AC-FPS
January 4 – January 18, 2014	None Detroit,MI	January 14, 2014	$9,985	Wire	x6750 AC-FPS
		January 21, 2014	$7,000	Cash	x4798 Hansen personal
February 17 - February 26, 2014	None Seattle,WA	February 26, 2014	$1,000	Cash	x4798 Hansen personal
		February 28, 2014	$5,000		
		March 11, 2014	$1,000		
		March 17, 2014	$800		
March 19 – March 26, 2014	None Seattle,WA	March 26, 2014	$9,900	Cash	x0702 Nuvestack
		March 27, 2014	$9,900		
			$1,000		x4798 Hansen personal
		March 31, 2014	$6,400		
April 20- April 26, 2014	None Seattle,WA	April 30, 2014	$4,000	Cash	x0702 Nuvestack
		May 5, 2014	$900		x4798 Hansen personal
		May 21, 2014	$3,000		
June 4- June 13, 2014	None Seattle,WA	June 11, 2014	$7,985	Wire	x6750 AC-FPS
		June 13, 2014	$5,000	Cash	x4798 Hansen personal
		June 17, 2014	$1,300		
		June 20, 2014	$1,000		
		June 30, 2014	$2,000		
TOTAL:			**$168,625**		

62. After his interdiction by CBP on July 9, 2014, HANSEN began declaring U.S. currency on a regular basis upon his return from the PRC. HANSEN's travel to the PRC from June 2014 through December 2015 similarly coincided with large cash deposits to HANSEN's personal and business accounts, as set forth in Table 2 below:

TABLE 2: July 2014 - December 2015 Travel from the PRC / Some Large Currency Declarations / Deposits					
Travel Dates	**Customs Declaration**	**Deposit Date**	**Amount**	**Type**	**Bank Account**
June 30 - July 9, 2014	$19,222 in Detroit, MI (Form Filed)	July 10, 2014	$9,000	Cash	x4798 Hansen personal
		July 11, 2014	$2,500		x4892 K.H. personal
		July 17, 2014	$1,000		x4798 Hansen personal
		July 18, 2014	$1,800		x4892 K.H. personal
August 27- September 6, 2014	$4,000 in Seattle, WA	September 5, 2014	$9,985	Wire	x6750 AC-FPS
September 17- October 1, 2014	None Portland, OR	October 1, 2014	$7,500	Cash	x4798 Hansen personal
October 15- October 29, 2014	$27,775 in Seattle, WA (Form Filed)	October 30, 2014	$5,000	Cash	x1730 Hansen personal
			$8,000		x4798 Hansen personal
		November 7, 2014	$1,500		
November 15- November 22, 2014	None Seattle, WA	November 24, 2014	$5,000	Cash	x6750 AC-FPS
			$2,000		x1730 Hansen personal
December 15- December 20, 2014	$30,000 in Seattle, WA (Form Filed)	December 22, 2014	$1,000	Cash	x4892 K.H. personal
			$9,000		x6750 AC-FPS
		December 23, 2014	$6,000		
		January 15, 2015	$1,500		x1730 Hansen personal
January 26 – February 5, 2015	$19,650 in Detroit, MI (Form Filed)	February 9, 2015	$1,000	Cash	x4798 Hansen personal
		February 26, 2015	$6,500		x1730 Hansen personal
February 27 – March 11, 2015	None Seattle, WA	March 18, 2015	$5,000	Cash	x1730 Hansen personal
April 6 – April 16, 2015	$30,040 in Seattle, WA (Form Filed)	April 17, 2015	$5,000	Cash	x4798 Hansen personal
			$6,800		x1730 Hansen personal
		April 27, 2015	$4,500		
		May 4, 2015	$2,000		x4798 Hansen personal
June 4 – June 9, 2015	None Seattle, WA	June 10, 2015	$5,000	Cash	x1730 Hansen personal
		June 22, 2015	$1,700		x6750 AC-FPS
			$1,592		x1963 Fahodie for Friends
July 21 – July 26, 2015		July 27, 2015	$5,000	Cash	x1730 Hansen personal
		July 30, 2015	$5,000		x6750 AC-FPS

	$20,700 in San Fran, CA (Form Filed)	August 10, 2015	$3,000		x1730 Hansen personal
		August 11, 2015	$1,008		x4798 Hansen personal
		August 24, 2015	$3,300		
August 16 – August 27, 2015	$20,267 in Seattle, WA (Form Filed)	August 28, 2015	$7,000	Cash	x1730 Hansen personal
		September 2, 2015	$2,500		
		September 3, 2015	$2,900		x4798 Hansen personal
		September 14, 2015	$3,000		x1730 Hansen personal
December 5 - December 14, 2015	$53,000 in Seattle, WA (Form Filed)	December 14, 2015	$8,000	Cash	x1730 Hansen personal
			$8,000		x4798 Hansen personal
		December 15, 2015	$7,400		x6750 AC-FPS
		December 16, 2015	$1,000		x4892 K.H. personal
		January 6, 2016	$2,900		x4798 Hansen personal
Total:			**$169,885**		

63. In conversations with law enforcement officials and others, HANSEN offered varying explanations regarding the source of his cash. For example, HANSEN claimed to CBP and FBI on at least one occasion that the cash related to the sale of surplus inventory and equipment following the 2013 closing of H-11 Beijing. However, in March of 2015, HANSEN told the FBI that he no longer had surplus inventory and equipment to sell in the PRC. When questioned by CBP about cash carried into the U.S., HANSEN never provided any documentation to confirm the sale of any surplus inventory or equipment from H-11 Beijing. As Tables 2 and 3 illustrate, HANSEN continued to bring significant sums of cash into the U.S. even after he advised CBP officers and FBI agents that little or no H-11 inventory or equipment remained to sell.

64. After receiving scrutiny by CBP regarding his pattern of carrying cash into the U.S. following trips to the PRC, HANSEN developed another method to transfer U.S. currency to his U.S. bank accounts using credit cards. During a phone call with a business associate on or about June 10, 2016, HANSEN stated that he found "another way" to move money out of the PRC. HANSEN explained that the PRC government places an annual limit of $50,000 per individual to transfer funds out of the PRC. To avoid the $50,000 limit, HANSEN further explained that an

individual could transfer funds out of the PRC using credit cards.

65. Emails confirm that, as early as March of 2016, HANSEN transferred money from the PRC using Visa cards with the assistance of Amy and Robert. The emails containing Visa card numbers included references such as "for Ron," "Ron's money," and "Money In from RH." Amy provided the Visa card numbers to both HANSEN and an accountant. Thereafter, at HANSEN's direction, the accountant processed the Visa card transactions through U.S.-based merchant accounts and then transferred the funds to HANSEN's personal and business accounts, as demonstrated in examples detailed below.

66. HANSEN traveled to the PRC on July 17, 2016, and he returned to the U.S. on July 23, 2016. HANSEN did not declare any currency at the airport. When questioned by CBP, HANSEN admitted carrying $9,970, an amount just under the reporting threshold. HANSEN told CBP officers that he would no longer carry currency across the border and that he would instead have money sent to him via Visa card transactions. HANSEN told CBP the Visa card transactions would involve a 3% fee, but he would rather pay the fee than be interviewed by CBP. On or about July 24, 2016, Amy sent an email to HANSEN and the accountant stating that there was "USD15,000 in this visa card for Ron." On July 27, 2016, the accountant processed the $15,000 Visa card transaction through the Nuvestack merchant account.

67. HANSEN traveled to the PRC on December 3, 2016, and he returned to the U.S. on December 10, 2016. On or about December 12, 2016, in a telephone conversation with the accountant, HANSEN described how he directed Amy and Robert to send $49,000 to the U.S. in increments of $10,000, $10,000, $15,000, and $14,000. On or about December 9, 2016, December 14, 2016, and December 22, 2016, Amy sent emails to HANSEN and the accountant with subject lines "Ron's money" and "third part of Ron's money." At HANSEN's direction,

the accountant processed $49,000 total in Visa card transactions through the Nuvestack merchant account.

68. On February 28, 2017, HANSEN told the CHS that the MSS always pays him in cash and he gives the cash to Amy and Robert to wire to him. HANSEN also told the CHS that he sometimes carries cash but he has to declare it if it is over $10,000.

69. HANSEN traveled to the PRC on May 11, 2017, and he returned to the U.S. on May 16, 2017. On or about May 17, 2017, HANSEN spoke with Robert by telephone. Robert stated that HANSEN could access the money the following night. Robert said that he could only deposit 5,000 U.S. dollars each day in the PRC, and it takes three days to deposit 15,000 U.S. dollars. On or about May 18, 2017, Amy sent an email to HANSEN and the accountant with subject line "money for Ron," notifying them of the availability of $15,000 "for Ron" on a Visa card. On or about May 19, 2017, the accountant processed the $15,000 Visa card transaction through the Nuvestack merchant account.

70. HANSEN traveled to the PRC on July 11, 2017 and he returned to the U.S. on July 18, 2017. On or about July 19, 2017, Amy sent an email to HANSEN and the accountant stating that "there is USD9000 for Ron on this Visa card." On or about July 20, 2017, the accountant processed the $9,000 Visa card transaction through the Nuvestack merchant account.

71. HANSEN traveled to the PRC on September 21, 2017, and he returned to the U.S. on September 28, 2017. On or about September 28, 2017, HANSEN wrote in an email to a friend in the PRC, "I have attached the Bank Information for the AC-FPS Business Group. Thank you. Hope to see you soon in Utah. Ron Hansen, CEO | AC-FPS Business Group." The friend responded, "OK." On September 29, 2017, bank records show that a wire originating from the PRC in the amount of $9,985 posted to the AC-FPS business account. On or about October 2,

2017, HANSEN, on a telephone call with a Nuvestack employee, explained the delay in paying the Nuvestack employee. HANSEN explained that the money was not "here" yet because "they've gotta put some money in the bank . . . then put some money on a credit card that I can swipe here because the money's coming from Asia." On or about October 4, 2017, Amy sent an email to the accountant and HANSEN stating there was "USD30000 in this visa card for Ron." On or about October 6, 2017, the accountant processed the Visa card through the Nuvestack merchant account.

72. HANSEN traveled to the PRC on November 16, 2017, and he returned to the U.S. on November 21, 2017. On or about November 16, 2017, during a telephone call, a business partner asked HANSEN to repay a $50,000 loan. During a later call, HANSEN stated that he could not produce a $50,000 lump sum payment, but "there are some things aligning." HANSEN stated he would probably get $10,000 to the business partner the following week. On or about November 22, 2017, HANSEN received a $27,985 wire originating from the PRC in his AC-FPS business account from the same friend referenced above. On or about November 22, 2017, HANSEN transferred $10,000, through the Nuvestack business account, to this business partner.

73. HANSEN traveled to the PRC on December 14, 2017, and he returned to the U.S. on December 19, 2017. On or about December 22, 2017, Amy sent an email to HANSEN about transferring money to HANSEN. Bank records show that on December 27, 2017, and January 3, 2018, two Visa card transactions were received in the Nuvestack business account in the amounts of $10,000 and $13,000 respectively.

74. Between July of 2016 and June 2, 2018, more than $200,000 was processed through the Nuvestack merchant account from PRC bank-issued Visa cards provided by Amy and Robert.

For tax year 2016, despite receiving approximately $90,000 through the Nuvestack merchant account using Amy and Robert's Visa cards, Nuvestack failed to file any corporate tax filings with the Internal Revenue Service.

75. For the merchant transactions, wires, and cash deposits described below in Table 3, HANSEN used the majority of the funds to benefit himself, his family members, and other entities, such as Nuvestack and AC-FPS, in which HANSEN held a vested financial interest. Bank records confirm that HANSEN did not transfer those funds to H-11 or use the funds in a way that benefitted H-11. Table 3 illustrates the methods HANSEN employed to transfer U.S. currency from the PRC to the U.S., after scrutiny by CBP in December of 2015:

TABLE 3: March 2016 - April 2018 No Large Currency Declarations / Cash, Card, and Wire Deposits					
Travel Dates	**Customs Declaration**	**Deposit Date**	**Amount**	**Type**	**Account**
March 9 – March 19, 2016	None Seattle,WA	March 21, 2016	$5,500	Cash	x1730 Hansen personal
		March 22, 2016	$9,500	Card	x8498 H-11 Digital Forensics
		March 28, 2016	$10,400		
May 7 – May 14, 2016	None Seattle,WA	May 19, 2016	$10,000	Card	x8498 H-11 Digital Forensics
			$5,000	Cash	x1730 Hansen personal
July 12 - July 23, 2016	$9,970 Seattle,WA	July 25, 2016	$8,500	Cash	x4798 Hansen personal
		July 27, 2016	$15,000	Card	x4721 Nuvestack
September 15 – September 24, 2016	$2,000 Seattle,WA	September 23, 2016	$10,000	Card	x4721 Nuvestack
		September 26, 2016	$2,000	Cash	x4798 Hansen personal
		September 28, 2016	$10,000	Card	x4721 Nuvestack
		September 29, 2016	$6,000		
December 3 – December 10, 2016	None Seattle,WA	December 12, 2016	$10,000	Card	x4721 Nuvestack
		December 13, 2016	$10,000		
		December 16, 2016	$15,000		
		December 19, 2016	$1,000	Cash	x4798 Hansen personal
		December 23, 2016	$14,000	Card	x4721 Nuvestack
	None Seattle,WA	February 21, 2017	$2,000	Cash	x4798 Hansen personal

February 9 – February 18, 2017		February 22, 2017	$19,000	Card	x4721 Nuvestack
April 9 – April 17, 2017	$2,500 Seattle,WA	April 18, 2017	$16,000	Card	x4721 Nuvestack
			$2,500	Cash	x4892 Kameron/Shelley
May 11 – May 16, 2017	$2,500 Seattle,WA	May 17, 2017	$2,500	Cash	x1551 Electrolytic Minerals
		May 19, 2017	$15,000	Card	x4721 Nuvestack
		May 26, 2017	$1,250	Cash	x1551 Electrolytic Minerals
July 11 – July 18, 2017	None Seattle,WA	July 19, 2017	$1,500	Cash	x4892 Kameron/Shelley
		July 20, 2017	$9,000	Card	x4721 Nuvestack
September 21 – September 28, 2017	$6,000 Seattle, WA	September 28, 2017	$6,000	Cash	x4798 Hansen personal
		September 29, 2017	$9,985	Wire	x6750 AC-FPS
		October 6, 2017	$30,000	Card	x4721 Nuvestack
November 16 – November 21, 2017	None Seattle,WA	November 21, 2017	$3,000	Cash	x4798 Hansen personal
		November 22, 2017	$27,985	Wire	x6750 AC-FPS
December 14 – December 19, 2017	$4,600 Seattle,WA	December 20, 2017	$3,000	Cash	x6750 AC-FPS
		December 27, 2017	$10,000	Card	x4721 Nuvestack
		January 3, 2018	$13,000	Card	x4721 Nuvestack
January 19 - January 24, 2018	$1,400 Seattle,WA	January 25, 2018	$500	Cash	x6750 AC-FPS
			$17,985	Wire	x6750 AC-FPS
March 2 - March 6, 2018	None Seattle,WA	March 7, 2018	$1,200	Cash	x6750 AC-FPS
			$17,960	Wire	x6750 AC-FPS
April 5 to April 10, 2018	None Seattle,WA	April 10, 2018	$1,000	Cash	x4798 Hansen personal
		April 12, 2018	$17,990	Wire	x6750 AC-FPS
		April 23, 2018	$1,000	Cash	x4798 Hansen personal
April 23 to April 28, 2018	None Seattle,WA	May 2, 2018	$21,985	Wire	x6750 AC-FPS
		May 4, 2018	$5,000	Cash	x6750 AC-FPS
Total:			**$398,240**		

76. Tables 1-3 summarize some, but not all, of the U.S. currency HANSEN declared to CBP or funds deposited into U.S. bank accounts contemporaneous with his travel from the PRC. From May of 2013 to the date of the Indictment, HANSEN received not less than $800,000 in funds originating from the PRC.

Export Control

77. On August 17, 2001, pursuant to the International Emergency Economic Powers Act (IEEPA), the President issued Executive Order 13,222, which declared a national emergency with respect to the unusual and extraordinary threat to the national security, foreign policy and economy of the United States in light of the expiration of the Export Administration Act, 50 App. U.S.C. §§ 2401-2420, which lapsed on August 17, 2001. 66 Fed. Reg. 44,025 (Aug. 22, 2001). While in effect, the EAA regulated the export of goods, technology, and software from the United States. Pursuant to the provisions of the EAA, the Department of Commerce (DOC) through the Bureau of Industry and Security (BIS) promulgated the Export Administration Regulations (EAR), 15 C.F.R. §§ 730-774, which contained restrictions on the export of goods, such as software with cryptoanalytic capability, outside of the United States, consistent with the policies and provisions of the EAA. *See* 15 C.F.R. § 730.2. Accordingly, the President ordered that the EAR's provisions remain in full force and effect despite the expiration of the EAA. Presidents have issued annual Executive Notices extending the national emergency declared in Executive Order 13,222 from the time period covered by that Executive Order through the present. *See*, e.g., 82 Fed. Reg. 39,005 (Aug. 18, 2017).

78. The Commerce Control List, published at 15 C.F.R. §774, listed the most sensitive items subject to the EAR. Items on the Commerce Control List were categorized by an Export Control Classification Number ("ECCN"), which contained information about the specific export

controls applicable to that ECCN. Depending on the applicable export control, destination, end use, and end user, DOC-BIS required an exporter to obtain a license in order to export certain items.

79. Under IEEPA and the EAR, willfully exporting, conspiring to export, attempting to export, or aiding and abetting the export from the U.S. of any item subject to the EAR that required a license without first obtaining the license from DOC constituted a crime.

Sumuri Recon Software

80. Sumuri LLC (Sumuri), a U.S. company located in Delaware, provided digital forensic training, software, hardware, and services. Sumuri manufactured the Recon Mac OS X Forensics with Paladin 6 software (Sumuri Recon software). That software contained cryptographic capability. By at least June 1, 2016, the Sumuri Recon software received an ECCN of 5D002.c.1. As a commodity controlled for anti-terrorism and national security reasons, the EAR prohibited the export of that controlled commodity to the PRC without a valid export license from the DOC-BIS.

81. On or about November 29, 2016, Amy requested that HANSEN purchase the Sumuri Recon software and bring it to her in the PRC. On or about December 12, 2016, HANSEN purchased the Sumuri Recon software for $1,717.95 purportedly on behalf of Nuvestack Inc., a U.S. company. On or about December 12, 2016, HANSEN directed an associate to ship the Sumuri Recon software to Amy in the PRC. On or about December 23, 2016, in an email message to HANSEN, Amy confirmed receipt of the Sumuri Recon software. HANSEN previously dealt with DOC-BIS and knew of the licensure requirement for export-controlled products. HANSEN did not obtain the requisite license to export the Sumuri Recon software to the PRC.

Vound Intella Software

82. Vound LLC (Vound), a U.S. company located in Colorado, provided products related to forensic search, e-discovery, and information governance. Vound manufactured the Intella 100 software.

83. For the export of any commodity valued at or above $2,500, the EAR required the exporter to complete an Electronic Export Information form (EEI), previously known as Shipper's Export Declaration (SED), in the Automated Export System (AES). Among other things, that form required the exporter to list the accurate value of the commodity (15 C.F.R. § 30). Electronic filing through the AES strengthened the U.S. government's ability to prevent export of certain items to unauthorized destinations and to unauthorized users.

84. On or about December 23, 2016, Amy requested that HANSEN purchase the Intella 100 Software and bring it to her in the PRC. On or about January 8, 2017, HANSEN purchased the Intella software from Vound for $3,030.00. After purchasing the software, HANSEN represented to the Vound sales manager that Nuvestack Inc. would be the end user of the product. Thereafter, HANSEN directed an associate to ship the Intella software to Amy in the PRC, which the associate did on or about January 19, 2017. At the request of Amy and with HANSEN's knowledge, HANSEN's associate listed the value of the product on the shipping documentation at $50.00, which HANSEN well knew to be false. HANSEN previously exported other products from the U.S. whose value exceeded $2,500. On those occasions, HANSEN submitted the requisite form, confirming that he knew of the disclosure requirement. HANSEN did not complete the EEI form regarding the export of the Intella software nor did he direct his associate to do so.

The Confidential Human Source and Attempted Espionage

85. As a routine investigative technique, the FBI enlists the participation of confidential human sources (CHS) to assist in investigations.

86. On May 24, 2016, HANSEN met with two former DIA associates for lunch in San Antonio, Texas. After lunch, HANSEN continued to speak to one of the DIA associates, inquiring about DIA sources and methods of operation. During the conversation, HANSEN disclosed that the MSS approached him. He also described his meetings with the FBI and stated that he "had to give the MSS something to keep stringing them along," while waiting for the FBI to make a decision about his offer to work as a "double agent."

87. Based on HANSEN's statements, the DIA associate filed a suspicious incident report. Thereafter, with DIA approval, the associate agreed to assist the FBI in its investigation by acting in the capacity of a CHS. At the time, the CHS worked as a DIA case officer.

88. Between 2016 and 2018, the CHS spoke to HANSEN several times. During those conversations, HANSEN disclosed ongoing contact with the MSS, including in-person meetings with senior MSS officers during his trips to the PRC. HANSEN stated that he performed consulting work for the MSS. HANSEN further stated that he sold computer forensic products to the PRCIS for which they "grossly overpaid" him in cash.

89. In October of 2016, HANSEN told the CHS that the MSS was still willing to pay him $300,000 a year to do consulting work. HANSEN related that the MSS asked him to write white papers on cell phones. HANSEN also said the MSS asked him about the views of various U.S. politicians regarding the PRC.

90. In February of 2017, HANSEN told the CHS that he attended intelligence and military conferences for the MSS. HANSEN stated that while none of the information at the conferences

was classified, the MSS could not obtain the same information as HANSEN because the MSS would not have the same access to high-ranking military officials as HANSEN did.

91. In March of 2018, HANSEN sent the CHS a copy of certain materials that he retained from his time as a U.S. government contractor. HANSEN asked the CHS to search for the information in intelligence reporting to determine how, if at all, the government used it. The materials that HANSEN sent to the CHS remained classified.

92. In March of 2018, HANSEN told the CHS that he met with a senior MSS intelligence officer during his March trip to the PRC. HANSEN discussed areas of interest expressed by the MSS intelligence officer about U.S. positions related to North Korea, South Korea, and the PRC. HANSEN asked the CHS to search intelligence reporting for information on a specific issue HANSEN described regarding North Korea. HANSEN also suggested he could act as a conduit to pass information to the MSS.

93. In April of 2018, shortly before HANSEN travelled again to the PRC, HANSEN discussed with the CHS his ability to facilitate the sale of national defense information to the PRCIS, saying he would meet with the MSS during his April trip to the PRC and assess their interest in information the CHS could obtain and provide. HANSEN discussed with the CHS ways to conceal their meetings and activities in the U.S. to avoid detection of their intent to sell national defense information to the PRCIS.

94. Later in April of 2018, HANSEN again met with the CHS shortly after returning from the PRC. During the meeting, HANSEN discussed the details of how he and the CHS might sell national defense information to the PRCIS. HANSEN advised the CHS regarding the type of information the PRCIS would find useful, and HANSEN advised the CHS how to record and transmit classified information without detection. HANSEN further suggested that the CHS

create notes related to the content of any classified material that the CHS would pass to HANSEN. HANSEN also discussed the possibility of the CHS doing a debriefing with the PRCIS in Canada or Mexico. HANSEN asked what amount of compensation the CHS would require for providing such information. HANSEN advised that the PRCIS might pay up to $200,000 if the CHS could deliver the "China ops plan," the operations plan of the United States military regarding potential military intervention with China. HANSEN explained how the CHS could hide and launder any funds received from the PRCIS, and HANSEN offered to help launder the money. On multiple occasions during the conversation, HANSEN asked whether the CHS was recording the meeting or "setting [HANSEN] up to go to jail." At the end of the meeting, HANSEN discussed using an application that provides encrypted communication for their future interaction.

95. In early May of 2018, after learning of the CHS' unavailability to meet prior to HANSEN's intended travel to the PRC on May 31, 2018, HANSEN suggested he could delay his travel to the PRC to a later date in order to accommodate the CHS' availability.

96. HANSEN subsequently made plans to travel from Salt Lake City to the PRC on June 2, 2018. He confirmed with the CHS that they would meet at a location close to the Seattle-Tacoma airport in Seattle, Washington, where HANSEN had a connecting flight to the PRC from the District of Utah.

97. On June 2, 2018, during his layover, HANSEN took a cab to meet the CHS at a pre-arranged location close to the Seattle-Tacoma airport. The CHS and HANSEN met in the CHS' car near the airport and drove to another location, also in the vicinity of the airport. The CHS brought two classified paper documents (the materials) to the meeting with HANSEN. The materials were classified at the SECRET level and marked accordingly.

98. At the outset of the meeting, HANSEN stated that he did not turn on his phone after he landed to insure that no one could track their location. The CHS informed HANSEN that he had materials to show HANSEN. HANSEN initially responded to this news by stating that he did not want to physically take the materials on his pending trip to the PRC. However, HANSEN later indicated that they should give his contacts in the PRCIS something to ensure that they would continue to work with the CHS and HANSEN in the future.

99. The CHS brought the materials in a concealment device. The CHS offered the materials in the device to HANSEN, who attempted to open the device but could not. The CHS then took the device back, opened the device, and asked HANSEN if he wanted to see the materials. HANSEN stated that he did and HANSEN then accepted the materials from the CHS.

100. During the majority of their two-hour meeting, HANSEN possessed the materials and reviewed them. HANSEN asked the CHS specific questions about the content of the materials. While reviewing the materials HANSEN stated that each paragraph of the materials would be worth a separate ten-minute conversation with the PRCIS. At one point, the CHS asked HANSEN how he would remember all the details of their discussion and HANSEN stated that he would remember the highlights. The CHS observed HANSEN take hand-written notes during their conversation.

101. The CHS and HANSEN also discussed how the CHS should procure and store documents that the CHS would obtain in the future for the PRCIS. HANSEN advised that the CHS should buy a computer and scanner and take steps to move the materials into a digital format. He also suggested that the CHS cut a hole in a nearby tree and hide materials in that location.

102. HANSEN also informed the CHS that the PRCIS would have to vet the CHS.

HANSEN asked for the CHS' date of birth, email addresses, employment locations, social media accounts, and information about the CHS' family members to provide to the PRCIS to facilitate the vetting process.

103. HANSEN told the CHS that he would not receive money after this trip to the PRC. However, he advised the CHS that he would arrange for the CHS to receive payment after his next trip to the PRC later in June. HANSEN stated he would arrange for his contacts in the PRC to give the money to one of HANSEN's business associates in the PRC who would then wire the funds to one of HANSEN's businesses. HANSEN would then have the funds "expensed" and arrange for them to be sent to the CHS.

104. After their meeting, the CHS dropped HANSEN off at a location close to the Seattle-Tacoma airport. HANSEN indicated that he would take his hand-written notes and incorporate them into an existing document. HANSEN then walked approximately one block from the drop-off location toward the entrance to a pedestrian bridge that accessed the airport when the FBI apprehended him.

105. When subsequently searched by the FBI agents, HANSEN had in his possession a single page of hand-written notes. Those notes included specific numbers corresponding to operational plans of the U.S. Army, contained in the materials that HANSEN received from the CHS. In his notes, HANSEN incorporated the operation numbers into Utah phone numbers in an attempt to mask their meaning. Additionally, the notes on the page included the CHS' date of birth, email addresses, and employment locations.

THE GRAND JURY FURTHER CHARGES THAT:

COUNT 1
18 U.S.C. § 794(a)
(Attempt to Gather or Deliver Defense Information)

106. Paragraphs 1-105 of this Indictment are incorporated by reference and re-alleged as though set forth fully herein.

107. On or about June 2, 2018, in the Northern Division of the District of Utah and elsewhere,

RON ROCKWELL HANSEN,

the defendant herein, did knowingly and unlawfully attempt to communicate, deliver and transmit directly and indirectly to a foreign government, to wit: the Government of the People's Republic of China, and representatives, officers, agents, employees, subjects and citizens thereof, documents and information relating to the national defense of the United States including documents marked SECRET//NORFORN that related to military readiness in a particular region, with intent and reason to believe that such documents and information will be used to the injury of the United States and to the advantage of any foreign nation; all in violation of 18 U.S.C. § 794(a).

COUNT 2
18 U.S.C. § 951
(Agent of a Foreign Government)

108. Paragraphs 1-107 of this Indictment are incorporated by reference and re-alleged as though set forth fully herein.

109. Beginning on a date unknown to the United States, but at least by April of 2013, and continuing through June 2, 2018, in the Northern Division of the District of Utah and elsewhere, the defendant,

RON ROCKWELL HANSEN,

did knowingly and willfully agree to act and did so act as an agent of a foreign government, to wit: the Government of the People's Republic of China, without prior notification to the Attorney General, all in violation of 18 U.S.C. § 951.

COUNTS 3-5
31 U.S.C. § 5332
(Bulk Cash Smuggling)

110. Paragraphs 1-109 of this Indictment are incorporated by reference and re-alleged as set forth fully herein.

111. On or about the dates listed below, in the Northern Division of the District of Utah and elsewhere, the defendant,

RON ROCKWELL HANSEN,

did, with intent to evade a currency reporting requirement under Title 31, United States Code, Section 5316, knowingly and unlawfully conceal more than $10,000.00, and transport and attempt to transport such currency from a place outside the United States to a place inside the United States, all in violation of 31 U.S.C. § 5332, as set forth below:

Count	Arrival Date (U.S.)	Customs Declaration	Deposit Date	Currency	Bank Account
3	November 26, 2013	None Seattle,WA	November 26, 2013	$9,000	x4798 WF Hansen personal
			November 29, 2013	$10,000	x6750 WF AC-FPS
4	March 26, 2014	None Seattle,WA	March 26, 2014	$9,900	x0702 WF Nuvestack
			March 27, 2014	$9,900	
				$1,000	x4798 WF Hansen personal
			March 31, 2014	$6,400	
5	July 9, 2014	$19,222 in Detroit, MI (Form Filed)	July 10, 2014	$9,000	x4798 WF Hansen personal
			July 11, 2014	$2,500	x4892 WF K.H. personal
			July 17, 2014	$1,000	x4798 WF Hansen personal
			July 18, 2014	$1,800	x4892 WF K.H. personal

WF: Wells Fargo

COUNTS 6-13
31 U.S.C. § 5324
(Structuring Monetary Transactions)

112. Paragraphs 1-111 of the Indictment are incorporated by reference and re-alleged as set forth fully herein.

113. Beginning on a date unknown to the United States, but at least by April 2013, and continuing until June 2, 2018, in the Northern Division of the District of Utah and elsewhere, the defendant,

RON ROCKWELL HANSEN,

did knowingly and for the purpose of evading the reporting requirements of Title 31, United States Code, Section 5313(a), and the regulations promulgated thereunder, structure and attempt to structure any transaction with one or more domestic financial institutions, as set forth below:

Count	Arrival Date (U.S.)	Customs Declaration	Deposit Date	Currency	Bank Account
6	November 26, 2013	None Seattle, WA	November 26, 2013	$9,000	x4798 WF Hansen personal
			November 29, 2013	$10,000	x6750 WF AC-FPS
7	March 26, 2014	None Seattle, WA	March 26, 2014	$9,900	x0702 WF Nuvestack
			March 27, 2014	$9,900	
				$1,000	x4798 WF Hansen personal
			March 31, 2014	$6,400	
8	October 29, 2014	$27,775 in Seattle, WA (Form Filed)	October 30, 2014	$5,000	x1730 BAF Hansen personal
				$8,000	x4798 WF Hansen personal
			November 7, 2014	$1,500	
9	December 20, 2014	$30,000 in Seattle, WA (Form Filed)	December 22, 2014	$1,000	x4892 WF K.H. personal
				$9,000	x6750 WF AC-FPS
			December 23, 2014	$6,000	
			January 15, 2015	$1,500	x1730 BAF Hansen personal
10	April 16, 2015	$30,040 in Seattle, WA (Form Filed)	April 17, 2015	$5,000	x4798 WF Hansen personal
				$6,800	x1730 BAF Hansen personal
			April 27, 2015	$4,500	
			May 4, 2015	$2,000	x4798 WF Hansen personal
11	July 26, 2015	$20,700 in San Fran,	July 27, 2015	$5,000	x1730 BAF Hansen personal
			July 30, 2015	$5,000	x6750 WF AC-FPS

		CA (Form Filed)	August 10, 2015	$3,000	x1730 BAF Hansen personal
			August 11, 2015	$1,008	x4798 WF Hansen personal
			August 24, 2015	$3,300	
12	August 27, 2015	$20,267 in Seattle, WA (Form Filed)	August 28, 2015	$7,000	x1730 BAF Hansen personal
			September 2, 2015	$2,500	
			September 3, 2015	$2,900	x4798 WF Hansen personal
			September 14, 2015	$3,000	x1730 BAF Hansen personal
13	December 14, 2015	$53,000 in Seattle, WA (Form Filed)	December 14, 2015	$8,000	x1730 BAF Hansen personal
				$8,000	x4798 WF Hansen personal
			December 15, 2015	$7,400	x6750 WF AC-FPS
			December 16, 2015	$1,000	x4892 WF K.H. personal
			January 6, 2016	$2,900	x4798 Hansen personal

WF: Wells Fargo, BAF: Bank of American Fork

And did aid and abet therein, all in violation of 31 U.S.C. § 5324 and 18 U.S.C. § 2.

COUNT 14
18 U.S.C. § 554
(Smuggling Goods from the United States)

114. Paragraphs 1-113 of the Indictment are incorporated by reference and re-alleged as set forth fully herein.

115. From on or about November of 2016 through January of 2017, in the Northern Division of the District of Utah and elsewhere, the defendant,

RON ROCKWELL HANSEN,

and others known and unknown, fraudulently and knowingly did attempt to export and send from the United States, any merchandise, article, and object contrary to any law and regulation of the United States, and did attempt to receive, conceal, buy, sell, and facilitate the transportation, concealment, and sale of such merchandise, article, and object, prior to exportation, knowing the same to be intended for exportation contrary to any law and regulation of the United States, and aided and abetted the same, to wit, HANSEN did cause to be exported from the United States Sumuri Recon software containing password recovery capability without first having obtained the required licenses from the United States Department of Commerce, and did aid and abet

therein, all in violation of 50 U.S.C. §§ 1702 and 1705, 18 U.S.C. §§ 554 and 2, and 15 C.F.R. § 764.2(b).

COUNT 15
18 U.S.C. § 554
(Smuggling Goods from the United States)

116. Paragraphs 1-115 of the Indictment are incorporated by reference and re-alleged as set forth fully herein.

117. From on or about December 23, 2016 through on or about January 19, 2017, in the Northern Division of the District of Utah and elsewhere, the defendant,

RON ROCKWELL HANSEN,

fraudulently and knowingly did attempt to export and send from the United States, any merchandise, article, and object contrary to any law and regulation of the United States, and did attempt to receive, conceal, buy, sell, and facilitate the transportation, concealment, and sale of such merchandise, article, and object, prior to exportation, knowing the same to be intended for exportation contrary to any law and regulation of the United States, and aided and abetted the same, to wit, HANSEN did cause to be exported from the United States Vound, Intella software with a falsified value, and did aid and abet therein, all in violation of 18 U.S.C. §§ 554 and 2, 13 U.S.C. § 305, 15 C.F.R. § 30.71, 15 C.F.R. § 764.2(g).

DATED this 20th day of June, 2018.

/s/
FOREPERSON of the GRAND JURY

JOHN W. HUBER
United States Attorney

ROBERT A. LUND
Assistant United States Attorney

EXHIBIT 2

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

UNITED STATES OF AMERICA,	:	Criminal Action Number 1:17-CR-154
versus	:	
	:	June 4, 2018
KEVIN PATRICK MALLORY,	:	
Defendant.	:	Volume IV of VIII

The above-entitled Jury Trial was continued before the Honorable Judge Ellis, United States District Judge.

A P P E A R A N C E S

FOR THE GOVERNMENT:

UNITED STATES ATTORNEY'S OFFICE
John T. Gibbs, Esquire
Colleen E. Garcia, Esquire
Jennifer K. Gellie, Esquire
US Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314

FOR THE DEFENDANT:

OFFICE OF THE FEDERAL PUBLIC DEFENDER
Geremy C. Kamens, Esquire
Todd Richman, Esquire
1650 King St
Suite 500
Alexandria, VA 22314

OFFICIAL UNITED STATES COURT REPORTER:

MS. TONIA M. HARRIS, RPR
United States District Court
401 Courthouse Square
Ninth Floor
Alexandria, VA 22314
703-646-1438

TABLE OF CONTENTS

TRIAL

WITNESSES

EXHIBITS

MISCELLANY

Q. This is the -- under the last bolded heading at the bottom.
A. Okay.
Q. At line 23?
A. Thank you.
Q. There is one word that has some black underlining under it. Did you add that, Ms. Morgan?
A. No, I did not.
THE COURT: Just a moment. Let me -- I have not yet found that.
MS. GELLIE: Certainly, Your Honor.
THE COURT: Oh, I see it. Yes, it's -- the underlining is by hand?
THE WITNESS: Correct.
THE COURT: Next question.
MR. KAMENS: Thank you, Your Honor.
BY MS. GELLIE:
Q. And underneath there's a bullet point at line 26 with the word in all capital letters. What does that word represent?
A. So that word is something we call a cryptonym. It's a word we use to disguise the actual name or hide the name of the actual asset or source that we are working with to help protect their identity. We also use cryptonyms for things like locations or the name of an activity to safeguard the most sensitive information.

Q. And what, if any, risk arises from the unauthorized disclosure of information in the bullet at line 26?
A. So in this case this means that source or that asset could be at risk of harm to them, their family, and their associates. That means in this country that would identify that they're working with our agency.
Q. Do you consider this intelligence information to relate to the national defense?
A. Yes, I do.
Q. Why?
A. Because it relates to the specific intelligence sources and methods and particular risks of threats to our country and our Homeland Security.
Q. Are there any specific risks to the United States should a foreign adversary gain access to this information?
A. Yes.
Q. What are those risks?
A. They learn about our capabilities, they learn about our intentions and our interests. And that means that country could then consider countermeasures or ways to stop making that information available to us.
Q. Are the examples you just discussed in this document the only classified portions of this document?
A. No.
Q. And did you determine any information in this document